Embargoed until release by the

House Armed Services Committee

Testimony

Before the

House Armed Services
Committee, Intelligence,
Emerging Threats and
Capabilities Subcommittee

Department of Defense
Information Technology,
Cybersecurity, and Information
Assurance

By

Ms. Lisa W. Hershman

Acting Chief Management

Officer

Department of Defense

February 26, 2019

UNCLASSIFIED

Testimony of Ms. Lisa W. Hershman, on Department of Defense Information Technology, Cybersecurity, and Information Assurance to the House Armed Services Committee, February 26, 2019

Thank you Chairman Langevin, Ranking Member Stefanik, and other members of this subcommittee for the opportunity to testify today on the Department's information technology (IT), cybersecurity, and information assurance. I am Lisa Hershman, the Acting Chief Management Officer (CMO) of the Department of Defense (DoD). I would like to begin today's hearing by outlining my roles, responsibilities and priorities, the Department's aggressive work to reform and modernize business operations through IT and business systems change, and the monumental changes in our management of data throughout the enterprise.

As the Acting CMO, it is my responsibility to deliver optimized business operations and shared services to assure the success of the National Defense Strategy (NDS). This responsibility is only made possible by the elevation of the CMO as the third in the Department and the critical authorities granted by you and your colleagues in the National Defense Authorization Act (NDAA) of Fiscal Year (FY) 2017. This law provided the CMO authority to direct the Principal Staff Assistants, Military Services, Combatant Commands, and remainder of the Defense Agencies and DoD Field Activities with regard to business operations.

My goal as Acting CMO aligns directly with the intent of the NDAA: efficiency for lethality. Efficiency for lethality is defined as reforming the Department's business processes, systems, and policies to gain increased effectiveness, higher performance, and reprioritized resources. Integrity and consistency of every measure is a cornerstone of our approach. I appreciate the work of the Office of Under Secretary of Defense for Comptroller (USD(C)) and the Military Departments for actively partnering to define standards for reform in execution and validate our efforts in the budget. Because of this effort, the Department has realized a total of $4.702 billion in programmed savings in FY17 and FY18, indicative of the success in reform efforts executed to date. However, reforming the business operations of the Department must not only be focused on financial savings, but also creating a sustainable, cultural impact. Through reform I aim to establish a culture of continuous improvement focused on results and accountability.

The Department's priorities of reform are based upon the framework defined by the FY19 NDAA, the President's Management Agenda, the senior leader Reform Management Group (RMG), and the first DoD-wide financial audit. While our reform efforts continue in the areas of civilian resource management, acquisition management, real estate management, logistics and supply chain management, contract management, and healthcare management, the President's Management Agenda, the RMG and the audit and identified business operations, IT infrastructure,

business systems, and data management as the most significant opportunity for improvement.

Our current IT and business systems environment is extremely complex. The Department currently maintains hundreds of business systems with ad hoc interconnectivity, thousands of data centers, hundreds of cloud efforts, and dozens of thousands of applications, with an IT and cyberspace budget of nearly $42 billion in FY18. These systems and infrastructures are managed by 65 Chief Information Officers (CIOs) throughout the Department with varying goals and performance metrics. This type of disparate management and duplication makes it extremely difficult for us to deliver an effective, innovative, or secure IT environment.

As the CIO for defense business systems in accordance with the FY18 NDAA, I consider it my responsibility to reverse this environment. I am developing the defense business systems strategy to ensure the development of integrated business processes through the Defense Business Enterprise Architecture. It is imperative to ensure the execution and enterprise management of business reform and associated business IT, and I am actively executing this in close coordination with Mr. Dana Deasy, the CIO.

We are executing IT reform efforts through several initiatives in four major areas. We are converging networks, service desks, and operation centers into a consolidated, secure, and effective environment capable of addressing current and future mission objectives. We are transitioning the Department to a cloud-enabled future, while standardizing IT commodity applications through commercial industry capabilities to deliver modernized services. We are unifying the Department's collaboration capabilities into a commercial cloud-enabled service. We are also modernizing coalition information sharing capabilities used by the Department and allied mission partners supporting global operations.

I would like to call your attention to the necessity of conducting business operations and systems reform. Despite the best efforts of software manufacturers, business systems represent a significant vector of cybersecurity vulnerabilities, from the business systems themselves to the supporting middle ware and operating systems. The number of vulnerabilities is a direct result of the sheer variety of software vendors, packages, releases, updates, patches, and configuration parameters which is then multiplied by the volume of software instances in use. The Department's sprawling portfolio of more than 1,800 business systems represents an uncomfortable level of exposure to cyber vulnerabilities.

In addition to these vulnerabilities, the Department historically under-invests in the modern tools and techniques for IT configuration management and IT asset

management, which are well proven as cybersecurity best practices in the commercial sector. These same business systems produce data that is of lower quality - less complete, less correct, less current, and less consistent - than what is ideal. In industry, high quality data is well established as a leading measure of high quality business systems, cybersecurity maturity, and business performance.

At a minimum, the Department's business systems should be operating at the same level as the commercial sector, if not higher. It is therefore imperative that we reform our business systems.

We are executing business systems reform by eliminating redundant systems, maximizing shared service delivery, and streamlining business operations. Through our initiatives we have made progress toward simplifying the IT landscape, reducing operational costs, through greater use of industry-proven enterprise services, and enabling business process integration.

As an example of our efforts in business operations and system reform, I would like to call attention to our Defense Civilian Human Resource Management System (DCHRMS) initiative. Through this initiative, we are aggressively driving change in how we manage the employee records of our civilians. Civilian job transfers within the Department occur roughly 40,000 times per year, with new employee records created each time an employee transfers. These records have been managed

by six separate systems that independently maintained the personnel records of our civilians. Through this reform initiative, the Department has rationalized policy and business processes to enable the consolidation of the six systems into one, cloud-based, software-as-a-service Human Capital Management capability. DCHRMS will be the first, single, authoritative, employee record system for all of our 900,000 civilians. DCHRMS will eliminate the unnecessary steps taken by human resource employees to create new employee records during transfers, and free up our human resource employees to focus on critical business deliverables, such as reducing time to hire. Most importantly, this consolidation will ensure a single, secure personnel record with one authoritative data source for all actions, removing hundreds of local copies of data yielding a material improvement in our cyber posture.

This initiative and others like it may seem commonplace when compared to the Department's operational missions, but are key enablers as we reduce duplication and inefficiency within the headquarters operations to achieve greater lethality and readiness.

As we execute these reforms, we remain ever mindful that the goal is delivery of secure, relevant, clean data to support both warfighting and business decisions, while IT infrastructures and business systems act as mere vehicles by which data travels.

The Department's historic operating environment poses many challenges to success in achieving this goal. The Department has traditionally been faced with a data analytics talent shortage, poor data quality, little to no data analytics policy, immature data analytics infrastructure, a complex data security environment, and outdated technology architectures for data analytics.

These challenges have not gone unrecognized by the members of the Armed Services Committees, and I want to personally thank you for supporting the data needs of the Department through the FY18 NDAA. This law provided the CMO with the framework to establish common enterprise data and data management and analytics as a shared service. To ensure data management had the full dedication it requires, I hired the Department's first Chief Data Officer (CDO), Mr. Michael Conlin.

The goal of establishing a CDO for the Department was not only to implement common enterprise data and data management and analytics as a shared service, but to create a lasting data-driven ecosystem. As outlined in my "Implementation Plan for Common Enterprise Data," this will require investments in people, processes, technology, and governance, and it will occur in four phases.

In the first phase of implementing common enterprise data, we began to understand the maturity of the Department's current data environment though pilot programs.

These pilot programs have allowed us to develop a repeatable business insight approach, implement proof of concept for the enterprise data analytics technical architecture, deploy a repository for common enterprise data, and define the data governance system.

To deploy a repository for common enterprise data, the CDO worked in conjunction with the Office of the USD(C) to develop the Defense Repository of Common Enterprise Data (DRCED) to be the shared-service platform for all common enterprise data. The DRCED is organized by a domain-oriented approach to include data management, audit findings, financial management, cost management, performance management, and readiness insights.

To define the data governance structure, the CDO established the Data Management and Analytics Steering Committee as the principal data governance body. This governance body is comprised of the chief management and financial officers of the Office of the Secretary of Defense, Military Departments, the Office of the Director of Cost Assessment and Program Evaluation, the Office of the CIO, the Office of the Principal Deputy Assistant Secretary of Defense for Readiness, and the Joint Staff J8 for Force Structure, Resources and Assessment.

We are now in the second phase of structuring and institutionalizing the Department's enterprise data governance and enterprise shared service analytics

capabilities. This includes developing a data science analytics training and career ladder, developing processes to maintain an enterprise data catalog and inventory, deploy artificial intelligence and machine learning, and developing the Department's Enterprise Data Strategy.

In the third phase, we plan to resolve organizational conflicts and eliminate differences in data approaches, leading to higher levels of constructive collaboration toward Department-wide goals. This norming phase includes establishing processes for integrated enterprise performance, cost, and budget reviews, completing automated cross domain security solutions, implementing data quality improvements, and accelerating the hiring of data scientists.

The fourth phase of this implementation will demonstrate the Department's ability to continually improve through a data-driven performance culture embedded in the business and mission processes. The Department will develop a performance evaluation assessment for the execution of the Department's Enterprise Data Strategy, and establish interoperability standards across lines of business.

 In sum, the implementation of common enterprise data will provide the Department improved data management practices, improved data security, an established analytics infrastructure to acquire, store, and analyze data, and enhanced enterprise decision-making throughout the Department. Through these efforts the end state of

our data environment will be a Department that makes decisions based on accurate, timely business data as opposed to internal boundaries and past experiences. This is a monumental shift in the way the Department conducts its business operations, and I am committed to ensuring the priority of data management in my role.

As Acting CMO and CIO of defense business systems, I am committed to leading business operations for the Department through innovative processes and services, data driven solution, and mission focused funding. It is imperative to our mission that we increase cybersecurity, modernize and standardize business processes, and decrease duplication of IT services throughout the Department. While I maintain this responsibility for data and business systems, I rely on my counterparts here with me today to be accountable. I entrust Mr. Dana Deasy as CIO to continually decrease duplication of IT services, and Brigadier General Dennis Crall as Deputy Principal Cyber Advisor to increase cybersecurity as an advocate for the implementation of the Department's Cyber Strategy.

Thank you for the opportunity to outline my roles, responsibilities, and priorities, and provide details of our work in reforming the Department's IT, business systems, and data management. I welcome your questions.

Lisa W. Hershman

Acting Chief Management Officer

Ms. Lisa W. Hershman is currently acting Chief Management Officer of the Department of Defense. Ms. Hershman has been serving as the Deputy Chief Management Officer of the Department of Defense.

Ms. Hershman is a recognized thought leader in business transformation who brings extensive private sector expertise to her service in the Department of Defense. She is the principal management officer for the Secretary and Deputy Secretary of Defense responsible for delivering optimized enterprise business operations to assure the success of the National Defense Strategy.

Ms. Hershman is responsible for ensuring that business transformation policies and programs are designed and managed to improve performance standards, efficiencies and effectiveness among the Office of the Secretary of Defense (OSD), the Services, Combatant Commands, and Defense Agencies and Field Activities. Additionally, she oversees the collection and management of common, enterprise-wide data sets to drive best decision-making throughout the Department.

Ms. Hershman is a charter member of the Office of Management and Budget's (OMB) Performance Improvement Council, and serves as the Performance Improvement Officer for the Department of Defense. She also serves as the Cross-Agency Priority goal leader for Category Management and Workforce of the 21st Century in support of the President's Management Agenda.

Prior to her service to the Department of Defense, Ms. Hershman was Founder and CEO of The DeNovo Group, a business transformation and process management consultancy. She is the former CEO of Hammer and Company, serving as the successor to the late Dr. Michael Hammer; the MIT icon, best-selling author and founder of the field of business process reengineering. Ms. Hershman is co-author of the internationally acclaimed business book, Faster Cheaper Better, with Dr. Hammer and has been featured in BusinessWeek, Forbes, Fox Business News, and Investors Business Daily.

In addition, Ms. Hershman served as Senior Vice President of Operational Excellence at Avnet, a global distributor of electronic components and technology systems. As the executive in charge of transformation and customer experience in 72 countries, her work was honored with the Avnet Corporate Chairman's Award. Ms. Hershman began her career with General Electric, where she managed a portion of the Seawolf submarine program.

Her civic engagement includes serving as the 2017 Chairwoman of the Scrum Alliance, Vice Chair of the Indiana Commission for Higher Education, and as a member of Ball State University's Miller School of Business Entrepreneurial Education Advisory Council.

Ms. Hershman earned her engineering and industrial distribution degree from Clarkson University and has studied innovation with MIT and IMD and finance with Cornell.